E-Safety Policy

Approval of the Governing Body

This document is a policy for:
e-Safety
at
Lambley Primary School.

It was developed/revised during the:
Autumn Term 2019.

It has been agreed and is supported by the teaching staff and the governing body.
We aim to review this policy during the:
Autumn Term 2020

Signature
Mr L Christopher
Headteacher

Lambley Primary School E-Safety Core Policy and Audit

E Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

The Core e-Safety Policy

This core e-safety policy provides the essential minimal school e-safety policy and has been based on guidelines from Kent, Stoke-on-Trent and Nottinghamshire LA's and the government.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students, encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Atom IT Services, including the effective management of Website filtering.
- National Education Network standards and specifications.

School e-safety policy

2.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, Bullying and for Child Protection.

- The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on local and national and guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.

2.2 Teaching and learning

2.2.1 Why are new technologies and Internet use important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2.2 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of effective knowledge location, retrieval and evaluation.

2.2.3 Pupils will be taught how to evaluate Internet content

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy, including 'fake news'.

2.2.4 Pupils will be taught how to stay e-safe

- Curriculum planning will include age appropriate opportunities to discuss, role play and learn about the benefits and risks offered by new technologies, such as e-mail, mobile phones and social networking sites.
- E-safety will be delivered as and when children are introduced to the areas of learning which need their awareness of e-safety to be heightened. Each class has designated lessons as outlined in the school's computing curriculum
- Pupils use of the Internet will be directed and for a specific curriculum purpose

2.3 Managing Internet Access

2.3.1 Information system security

- Virus protection will be updated regularly on all networked computers.
- School ICT systems capacity and security will be reviewed regularly.
- The main protection will be through a filtering system or 'firewall' operated by the chosen Internet service provider of Nottinghamshire County Council (ISP).

2.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain letters will be actively discouraged and the potential harm that can be caused will be included within e-safety learning.

2.3.3 Public Web published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number. **Staff or pupils' personal information will not be published.**
- E-mail addresses will be published carefully, to avoid spam harvesting.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications, including respect for intellectual property rights and copyright.

2.3.4 Web Publishing pupils' images and work

- Images, published to the web, that include pupils will be selected carefully and will only be published with parental approval
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published to the web.
- Pupil's work can only be published to the website with the permission of the pupil and parents.

2.3.5 Social networking and personal publishing

- The LA/school will block/filter access to social networking sites, except those specifically purposed to support educationally approved practice.
- Newsgroups will be blocked unless a specific use is approved.
- Staff and pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces often have age-restrictions and these should be adhered to.
- Staff and pupils should be advised not to publish specific and detailed private thoughts on social networking sites.
- Staff, governors and parents should both refer to our Code of conduct policies for further guidance in this area.

2.3.6 Managing filtering

- The school will work with Nottinghamshire 1C1N Managed Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, the URL must be reported to the school ICT Coordinator / Business Manager / e-Safety Coordinator, who will then contact the ICT Schools Service Desk (TEL: 0115 977 2010).
- Staff will set up access for pupils or visually check whenever pupils use the Internet for investigation or information search (Google – preferences –strict filtering / www.safesearchkids.com)

2.3.7 Managing remote teaching/video-conferencing

At present, we do not have the facilities to video-conference in school. However, when this is considered and appropriate step to take, the following guidelines will be considered:

The equipment and network

- Full IP videoconferencing will use the national educational or the schools' broadband network to ensure quality of service and security.
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the school Website.
- School videoconferencing equipment will not be taken off school premises without permission, since use over a non-educational network (e.g. the internet) cannot be monitored or controlled.

Users

- Pupils will ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age.
- Parents and guardians will agree for their children to take part in videoconferences.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.
- Only key administrators will be given access to the videoconferencing system, web or other remote control page available on larger systems.

Content

- When recording a videoconference lesson, written permission will be sought by all sites and participants. The reason for the recording is given and the recording of videoconference is clear to all parties at the start of the conference.
- Recorded material will be stored securely.

- If third-party materials are to be included, recordings will be checked that they are acceptable to avoid infringing the third party intellectual property rights.
- Dialogue will be established with other conference participants before taking part in a videoconference. If it is a non school site it is checked that they are delivering material that is appropriate for the class.

2.3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out and protocols established before use in school is allowed.
- Mobile phones ARE NOT allowed to be used in school by pupils. The sending of abusive or inappropriate text messages is forbidden.

2.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.4 Policy Decisions

2.4.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications, which includes internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- All staff must read and sign the '**Staff Information Systems Code of Conduct'** before using any school ICT resource.
- Throughout each Key Stage, access to the Internet will be demonstrated and supervised by the Teacher or Teaching Assistant of the class. They will then directly supervise access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Sanctions for inappropriate use will be drawn up and shared with staff and pupils.
- Staff must communicate through their school specific email account

2.4.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Nottinghamshire LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

2.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy will include:
    - informing parents or carers;
    - removal or restriction of Internet or computer access for a period.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

2.4.4 Community use of the Internet

At present, the wider school community does not require access to the internet through the use of the school computers. However, if in the future this is required, then a suitable approach to e-safety will be agreed.

2.4.5 Cyberbullying – Understanding and addressing the issues

While cyberbullying is likely to be low level in primary schools the age of pupils making proficient use of technology is ever decreasing. Therefore, the opportunities for pupils to bully or be bullied via technology, such as e-mail, texts or Social Media, are becoming more frequent.

As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding for future use. Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of cyberbullying.

As felt appropriate for the age and use of technology by the pupils:

- The school's anti-bullying & equality policy and/or school behaviour policy will address cyberbullying. Cyberbullying will also be addressed in ICT, PHSE and other relevant lessons and is brought to life through activities. As with other whole-school policies, all staff and young people will be included and empowered to take part in the process.
- Pupils, parents, staff and governors will all be made aware of the consequences of cyberbullying. Young people and their parents will be made aware of pupils' rights and responsibilities in their use of new technologies, and what the sanctions are for misuse.
- Parents will be provided with an opportunity to find out more about cyberbullying through: guidance for parent's, the CEOP website.

2.4.6 Cyberbullying - How will risks be assessed?

- The school will take all reasonable precautions to ensure against cyberbullying whilst pupils are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school computer will not occur. Neither the school, nor Nottinghamshire LA, can accept liability for inappropriate use, or any consequences resulting outside of school.
- The school will proactively engage with ALL pupils in preventing cyberbullying by:

- understanding and talking about cyberbullying, e.g. inappropriate use of e-mail, text messages;
- keeping existing policies and practices up-to-date with new technologies;
- ensuring easy and comfortable procedures for reporting;
- promoting the positive use of technology;
- evaluating the impact of prevention activities.

- Records of any incidents of cyberbullying will be kept and will be used to help to monitor the effectiveness of the school's prevention activities.

2.4.7 How will cyberbullying reports/issues be handled?

- Complaints of cyberbullying will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Evidence of offending messages, pictures or online conversations will be kept, in order to demonstrate to others what is happening. It can be used by the school, internet service provider, mobile phone company, or the police, to investigate the cyberbullying.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy include:
  - informing parents or carers;
  - removal of Internet/computer access for a period or banning of mobile phone in school.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with pupils at the start of each year and as the need arises.
- Pupils will be informed that network and Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- Pupils will be taught and directed to report any unacceptable use by other pupils to their teacher
- Pupils will be taught and directed to report any unacceptable materials, which they access by accident or mistake to their teacher

- **2.5.2 Staff and the e-Safety policy**
- All staff will be given the School e-Safety Policy and its application and importance explained.
- All staff will be informed that all computer and Internet use will be monitored. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

2.5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy through the sending of a letter, informing them briefly of the policy and asking for their signature as consent for their child to access the internet whilst at school.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged.

Version:	1
Date approved:	12.11.2019
Approved by:	FGB and C O'Hara Link Governor
Next review:	Nov 2020

Lambley Primary School

RULES FOR THE INTERNET AND E-MAIL

1 You must ask permission from a teacher before using the internet or e-mail
2 Do not access other peoples files
3 Never use your own discs, flash drives or CDs unless they have been checked by a teacher and you have permission
4 Always get your e-mail message checked by a teacher BEFORE you send it
5 Never give any personal information such as your name or address to people you do not know
6 Report anything which is unpleasant or suspicious to a teacher

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes (including online purchases), without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission, either on school computers or the laptop provided for me by the school.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Capitals: …… Date: ……

Accepted for school: …… Capitals: …….

E-mail and Internet Use Agreement

All schools must establish an e-mail and Internet use agreement for pupils covering the expectations the schools have of pupils using NCC's e-mail and Internet service in school. All pupils and their parents / guardians must be asked to read and sign the agreement.

A template for an E-mail and Internet Use Agreement

This e-mail and Internet agreement must be read through with your parent(s) / guardian(s) and then signed. You will be allowed e-mail and Internet access after this is returned to school.

- We expect all pupils to be responsible for their own behaviour in using the Internet and e-mail, just as they are anywhere else in school. This includes materials they choose to access, and language they use.
- Pupils using the Internet are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to their teacher, who will act on it accordingly.
- Pupils are expected not to use any rude language in their email communications and contact only people they know or those their teacher has approved. It is forbidden to be involved in sending chain letters.
- Pupils must ask permission before accessing the Internet.
- Pupils must not access other people's files unless permission has been given.
- Computers must only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet.
- No programs on disc or CD Rom should be brought in from home for use in school.
- In exceptional circumstances, homework completed at home may be brought in on disc but this will have to be virus scanned by the class teacher before use.
- Personal printing on the school network (e.g. pictures of pop groups/cartoon characters) is not permitted unless permission has been given.
- Personal information such as phone numbers and addresses must not be given out and arrangements must not be made to meet anyone unless this is part of an approved school project and has been approved by the Head Teacher.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to e-mail and the Internet resources.

I have read through this agreement with my child and agree to these safety restrictions.

Signed: _____ (Parent/Guardian)

Name of child: _____

Date: _____

Dear Parent,

Responsible use of e-mail and the Internet

I am sure you will have heard about some of the problems that can arise when young children use e-communication systems such as the Internet and e-mail - problems that range from bullying to the grooming of young children by adults.

The Internet is part of everyday life, brings a wealth of advantages, and we cannot ignore it. At the same time the school takes every precaution to ensure that your child is safe when using the Internet and e-mail at school. Although, at present, no children at school are provided with an email address.

In addition to the school taking its own precautions, we are aided by our colleagues at Atom IT who provide the Internet filtering service to the school to ensure that all children are as safe as possible when using the Internet and email at school.

The Internet filtering service restricts access to sites containing inappropriate content. All our screens are in public view and normally an adult is present to supervise.

No system is perfect, however, and you should be aware that it is not possible to remove entirely the risk of finding unsuitable material. We want to inform you of the rules which the children are expected to follow to help with our precautions.

I would ask you to look through these rules and discuss them with your child and then return the signed form to us at school.

If you would like to have a look at our full 'e-safety Policy', you will find it on the school website.

Yours faithfully

Mr Christopher
Head Teacher